Contactless Consumer Payments: A Look at Rules, Laws, and Regulations That Apply to Over-the-Air Communication of Consumers' Payment Information

Philip Keitel*

August 2010

This note summarizes a variety of rules that govern over-the-air communication of consumers' payment information, an essential ingredient to the functionality of contactless consumer payment instruments. These rules affect how those devices will be designed, how banks will deploy them, and which merchants are likely to accept them.

Contactless consumer payment instruments are devices based on infrared, Bluetooth, radio frequency identification (RFID), and near-field communication (NFC) technologies that permit consumers to make payments without swiping their cards or coming into physical contact with terminals at the point-of-sale. The prevalence of these payment instruments is growing in the United States: At present, tens of millions of contactless payment cards have been issued to U.S. consumers.[1] J.P. Morgan Chase alone has issued 30 million contactless payment cards,[2] and more than 150,000 point-of-sale terminals at merchants and service providers can accept contactless consumer payments.[3] With large-scale issuance of mobile phones with built-in contactless payment technology on the horizon,[4] and plans for widespread deployment of contactless debit cards in Canada,[5] contactless consumer payments may someday become ubiquitous in North America. The fundamental feature of contactless consumer payments is the over-the-air transmission of consumers' payment-related information. This note looks at the rules, laws, and regulations related to the transmission of consumers' payment-related information and how they apply to contactless payments.

While very little state or federal law is triggered by the over-the-air communication

of consumers' payment information (the subject of the section on Laws and Regulations, below),[6] and no case law exists on the topic, a number of rules nonetheless apply. These rules, and the contracts that enforce them, affect the physical make-up of contactless consumer payment instruments, determine the types of contactless payment instruments that consumers have (or will have) access to, and influence the behavior of both the banks that issue payment instruments and the merchants that accept them. This note highlights several such rules and their scope. These rules include technical specifications, payment association rules, and payment-industry-established data security protocols. In addition, this review looks at a Nevada law that incorporates payment-industry-established standards (related to the secure, over-the-air communication of payment information in particular), and Massachusetts regulations that address the communication of consumer payment information using wireless devices. This note also looks at financial institution examination guidelines that require financial institutions to vet providers of services associated with advanced payment technologies. This note concludes by observing that the communication of consumers' payment information over-the-air is a rapidly developing area that presents unique legal questions meriting close attention as consumers' use of contactless payments increases.

Technical Specifications, Electronic Payments Association Rules, and Payment-Industry-Established Data Security Protocols

Although little federal or state law (or regulation) applies to the over-the-air communication of consumers' payment information (the subject of the section on Laws and Regulations, below), a myriad of rules are nonetheless germane. These rules have been promulgated by various entities, including standard-setting organizations, payment networks, payment associations, and payment industry coalitions. The rules include technical specifications, payment association rules, and payment-industry-established data security protocols. They govern things like the physical make-up of contactless consumer payment instruments, how contactless payment instruments enter the marketplace, and how payments-related data is transmitted to or from these payment instruments. This section details these rules and their scope.

Technical Requirements

Similar to most technologies in the marketplace today, contactless consumer payments employ standard operating procedures and protocols established by various standard-setting bodies, which include the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), EMVCo, the Near Field Communication Forum (NFC Forum), and the Accredited Standards Committee X9 (ASC X9).[7] These procedures and protocols — embodied in technical requirements and operating standards — set ground rules for how contactless consumer payment instruments must operate. The rules are ultimately enforced through various contracts between payment networks, banks, merchant banks, and merchants. They provide key market participants, such as the manufacturers of contactless payment instruments and acceptance devices, with core specifications around which they can create interoperable technology.

At the heart of contactless consumer payments-related rules (and RFID-based payments in general) is a standard known as ISO/IEC 14443.[8] This standard (in parts 1-4)

defines the physical characteristics of proximity integrated circuit cards, or PICCs, and establishes protocols for communication between these cards and other devices, such as readers – called payment coupling devices, or PCDs, under the standard. In addition, related parts look at the physical characteristics of cards, radio frequency power and signal interference, initialization and anti-collision, and transmission protocol.[9]

Another standard, the EMV Contactless Communication Protocol Specification, is published by EMVCo, a joint venture between major payment networks American Express, JCB, MasterCard, and Visa. This standard establishes specifications for the manufacture of contactless payment instruments.[10] Essentially, the EMV Contactless Communication Protocol Specification allows payment system designers (such as manufacturers of contactless payment instruments, manufacturers of devices for accepting contactless payments, and financial institutions) a minimum set of functional requirements "to ensure correct operation and interoperability."[11] In other words, the EMV Contactless Communication Protocol Specification serves as a collective payment-network-interpretation of ISO/IEC 14443, an interpretation that must be followed in order to produce contactless cards for the U.S. market.

Compared to RFID-based payments technology, NFC-based payments technology has additional technical specifications beyond those outlined in ISO/IEC 14443 and the EMV Contactless Communication Protocol Specification.[12] Largely promulgated by the NFC Forum, the additional technical standards applicable to NFC-based payments address things like the type of connection that payments devices must establish, the format for the exchange of payments-related data, and the kind of information that can be stored on certain devices.[13]

While technical standards set by various standard-setting bodies provide the chief underlying set of rules that govern the physical make-up of contactless consumer payment instruments, there are additional rules that direct the design of these payment instruments and control how they enter the market. For example, major U.S. payment networks issue their own specifications around which contactless consumer payment instruments must be designed and require that instruments that interact with their networks be tested and approved before entering the marketplace.[14] For businesses that buy contactless payment technology, such as banks that want to buy contactless payment cards to issue to their customers, or merchants that want to purchase contactless payment device readers for the point-of-sale, major U.S. payment networks maintain lists of approved contactless consumer payments devices.[15]

Payment Association Rules

In May 2010, members of the major electronic payments association, the National Automated Clearing House Association, or NACHA,[16] approved the Mobile ACH Payments Rule. [17] The rule, which becomes effective January 1, 2011, permits ACH debit transfers that are initiated by or that involve communication sent over a wireless network to be submitted as "WEB" coded transactions. According to NACHA, the "rule will expand the definition of Internet-Initiated Entries (WEB) to include ACH debits authorized and/or initiated via wireless networks and require that those payments utilize the WEB Standard Entry Class (SEC) Code."[18] Essentially, this rule lays the foundation for

over-the-air origination by consumers of ACH transfers.[19]

Payment-Industry-Established Data Security Protocols

The Payment Card Industry Security Standards Council has established standards that govern how organizations hold and transfer consumer-payments-related information.[20] Two such standards are the Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA DSS). American Express, Discover Financial Service, JCB International, MasterCard Worldwide, and Visa have incorporated these standards into their data security compliance programs. Both standards contain provisions that relate to the over-the-air communication of consumers' payment information.[21] The PCI DSS requires "wireless environments connected to the cardholder data or transmitting cardholder data" to have "wireless vendor defaults [changed], including but not limited to default wireless encryption keys, passwords, and [simple network management protocol] community strings," and managers of these environments must "ensure wireless device security settings are enabled for strong encryption technology for authentication and transfer."[22] In addition, organizations that accept most bank-issued payment instruments must "install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment."[23] Similar to requirements of the PCI DSS, the PA DSS requires all users of payment applications that incorporate wireless technology to ensure that the wireless technology is "implemented securely."[24] This requires, for example, verification "that the wireless applications do not use vendor default settings and are configured in accordance with [the standard]," and verification of installation by vendors or appropriate parties of required firewalls.[25] Overall, these standards significantly influence the market for contactless consumer payment instruments by establishing compliance requirements for devices that accept contactless payment instruments, the networks that support such devices, and the transmission of payment-related information as part of settlement processes.

Laws and Regulations

This section looks at a provision of Nevada law that incorporates the PCI DSS, at Massachusetts regulations that address the communication of consumer payment information using wireless devices, and at Federal Financial Institutions Examination Council examination guidelines related to over-the-air communication of consumers' payment information.

Nevada Revised Statute chapter 603A

Under Nevada Revised Statute chapter 603A, consumers' "personal information," which includes a consumer's "account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account," must be handled in a manner that complies with the PCI DSS.[26] Section 603A.215 of the statute requires "data collector[s]"[27] doing business in Nevada, and that accept payment cards in connection with the sale of goods or services (this would include contactless payment cards), to "comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI

Security Standards Council or its successor organization," which, as the last section details, has several substantive requirements that concern the over-the-air transfer of consumer payment information.[28]

Massachusetts Office of Consumer Affairs and Business Regulation's Standards for the Protection of Personal Information of Residents of the Commonwealth

Pursuant to Massachusetts General Law, chapter 93H (a law related to data security and data security breaches),[29] the Massachusetts Office of Consumer Affairs and Business Regulation's "Standards for the Protection of Personal Information of Residents of the Commonwealth" establish "minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records."[30] Under these standards, every person, corporation, association, partnership, or other legal entity[31] that electronically[32] stores or transmits consumers' personal information (personal information includes a Massachusetts resident's debit or credit card number in combination with that resident's first name and last name or first initial and last name)[33] must have a written, comprehensive security program that covers computers and "any wireless system" used.[34] Such a program must, to the extent technically feasible, and in addition to a number of other requirements, provide for the "encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly."[35]

Federal Financial Institutions Examination Council Internet Technology Examination Handbook

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body that drafts standards, guidelines, principles, and model report forms for federal examination of financial institutions by federal banking regulatory agencies. The FFEIC has issued examination guidelines with provisions that relate to payment technologies capable of over-the-air communication of consumers' payment information. The *2010 Retail Payment Systems IT Examination Handbook* (the handbook) notes that "financial institutions offering advanced payment technologies [must] perform due diligence and vendor management as they would on any service provider."[36]

In addition, the handbook, in a section entitled Emerging Network Technologies, observes that "emerging payment systems rely upon, and may be integrated with, underlying network communication technologies and protocols. If not properly implemented, new and emerging network communication technologies may expose the payment device or system to additional vulnerabilities. This is particularly true with any network that relies upon broadcast technology to send and receive information. Even close proximity wireless devices, such as RFID, have been found to be vulnerable to eavesdropping at distances greater than they were designed for. Care should be taken to ensure that the underlying network communication technology has security appropriate to the information being transmitted. Currently, there are four types of short-range wireless connectivity technologies that can be used to connect payment devices to POS devices. These include: Infrared, RFID, NFC, and Bluetooth."[37]

Conclusion

Although contactless payment technology is believed to provide significant, important advantages over existing technology — such as the ability to increase the speed of transactions, the ability to provide greater protection for consumers' payments-related information,[38] or the ability to dynamically store and update important information related to particular transactions (such as warranty or reward program information)[39] — the types of contactless payment instruments that consumers will have access to and the methods of communicating consumers' payment-related information over-the-air are still developing. So too are the rules that govern these instruments and the over-the-air communication of consumers' payment information. As this development continues, stakeholders in electronic consumer payments should maintain an open dialogue with regulators to ensure that state and federal regulations do not unduly impair the development of a payment technology that can provide significant, important advantages over existing technology.

---

* The views expressed in this review are those of the author and not necessarily those of the Federal Reserve Bank of Philadelphia or the Federal Reserve System.

Thanks to George Kocur, senior lecturer, MIT Department of Civil & Environmental Engineering, for insights.

[1] Smart Card Alliance, "Issuer and Merchant Best Practices: Promoting Contactless Payments Usage and Acceptance," (September 2009), p. 4.

[2] Kate Fitzgerald, "After Half A Decade, Is 'Tap and Go' Tapped Out? Contactless-payment Development Is Languishing with Patchy Distribution and Tepid Marketing Some Five Years After Its Introduction, Although Some Bright Spots Beckon," *PaymentsSource* (March 1, 2010).

[3] See Smart Card Alliance (September 2009), p. 4.

[4] See Marianne Crowe, Marc Rysman, and Joanna Stavins, "Mobile Payments in the United States at Retail Point of Sale: Current Market and Future Prospects," Federal Reserve Bank of Boston Public Policy Discussion Paper No. 10-2 (May 17, 2010), p. 5, discussing business cases underlying mobile-phone-based payments. See also Julia Cheney, "An Examination of Mobile Banking and Mobile Payments: Building Adoption as Experience Goods?," Federal Reserve Bank of Philadelphia, Payment Cards Center Discussion Paper (June 2008), discussing the state of mobile payments and banking in 2008.

[5] See Daniel Wolfe, "Interac to Roll Out Contactless System," *American Banker* (June 18, 2010), noting that Canadian banks and the Canadian payment network Interac plan to widely deploy contactless debit cards in Canada in 2011 and are currently testing contactless debit card technology on a large scale.

[6] To be clear, a number of federal regulations presently govern one or more aspects of consumer payments, including, for example, Regulation E (which governs certain electronic fund transfers to and from consumers' accounts) and Regulation Z (which governs certain types of credit accounts), but no federal financial regulation presently governs the over-the-air transmission of consumers' payment information (although the underlying payment or transfer of funds may be regulated).

[7] ISO is a nongovernmental organization, made up of standard-setting bodies in 163 countries, that develops and publishes international standards to help establish a consensus about technology. Similarly, IEC is a global organization that "prepares and publishes international standards for all electrical, electronic and related technologies." EMVCo, currently owned by American Express, JCB, MasterCard, and Visa, sets specifications for chip-based payment instruments and administers testing and approval processes for evaluating compliance with specifications. The NFC Forum was formed in 2004 to "advance the use of Near Field Communication technology by developing specifications, ensuring interoperability among devices and services, and educating the market," and consists of 140 member organizations that include chip manufacturers, applications developers, financial institutions, and others. ASC X9, approved by the American National Standards Institute (ANSI), develops

standards and guidelines for the facilitation of banking operations, including consumer payments. See www.iso.org/iso/home.html, www.iec.ch/index.html, www.nfc-forum.org/aboutus/, www.emvco.com/default.aspx, and www.x9.org/home/, respectively (accessed July 16, 2010).

[8] A copy of the current standard is available for purchase at: ww.iso.org/iso/catalogue_detail.htm?csnumber=39693. Additional, preview information is available at: http://webstore.iec.ch/preview/info_isoiec14443-1%7Bed2.0%7Den.pdf.

[9] Although ISO/IEC 14443 and its related subparts concern "identification" cards, a number of consumer payments applications have been built using these specifications, and ISO/IEC 14443-compliant devices are often linked to an online account that can be funded via transfers from a consumer's account or line of credit. See, for example, the Massachusetts Bay Transportation Authority's Charlie Card Program, which uses MIFARE technology (technology produced by NXP semiconductors that is based closely on ISO/IEC 14443). Information on the Charlie Card is available at: www.mbta.com/fares_and_passes/charlie/.

[10] EMVCo, "EMV Contactless Specifications of Payment Systems: EMV Contactless Communication Protocol Specification," Version 2.0.1 (July 2009). A copy of the protocol is available for download at: www.emvco.com/specifications.aspx?id=21.

[11] See EMVCo (July 2009), p. 1.

[12] The NFC Forum notes that its implementation specifications must be incorporated "on top of" ISO/IEC 14443 and other specifications. *See* www.nfc-forum.org/resources/faqs#headSpecifications (accessed July 28, 2010).

[13] See www.nfc-forum.org/aboutnfc/ for more information about the NFC Forum, and www.nfc-forum.org/specs/spec_dashboard/ for a listing of specifications and the matters to which they relate (accessed July 28, 2010).

[14] See, for example, Visa, "Visa Contactless Payment Specifications: User Interface Guidelines, Version 1.0," (September 2008), p 1. But note that these specifications do "**not** specify actual requirements," merely general requirements that a device manufacturer can look to in designing devices for accepting contactless payments, because testing and approval of individual products is required by Visa.

[15] See, for example, MasterCard's approved PayPass product website: www.paypass.com/approved-products.html, and Visa, "Visa Approved Products Developed to Visa Contactless Payment Specification as of July 2010" (July 2010), pp. 1-17.

[16] Information about NACHA is available on its website: www.nacha.org/ (accessed July 29, 2010).

[17] Andrew Johnson, "New Rule Lays Foundation for Mobile ACH Payments," *American Banker* (June 21, 2010).

[18] NACHA, "Mobile ACH Payments," Herndon, VA (May 2010); available at: www.nacha.org/c/_content.cfm/AID/780/ (accessed July 29, 2010). For more information see NACHA, "Understanding the WEB Rules," (webinar) Herndon, VA (July 2010); available for purchase at: www.nacha.org/member-apps/index.cfm?action=events.events (accessed July 29, 2010).

[19] For a discussion of some of the ramifications of increased ACH traffic and of web-initiated transactions in particular, see Richard M. Todd, "Managing Risks in the ACH Network: Minneapolis Fed Study Uses FedACH Data to Identify Better Benchmarks," Federal Reserve Bank of Atlanta, Retail Payments Risk Forum Portals and Rails Blog (June 29, 2010); available at: http://portalsandrails.frbatlanta.org/.

[20] The Payment Card Industry Security Standards Council, founded in 2006, is responsible for several electronic payments-related security standards, including the Data Security Standard, the Payment Application Data Security Standard, and the Pin-Entry Device Requirements. For more information on the Payment Card Industry Security Standards Council, see www.pcisecuritystandards.org/about/index.shtml (accessed July 29, 2010).

[21] These standards by-and-large govern devices that read consumer payment instruments and both store and transmit consumer-payments-related information, and not the physical make-up of contactless consumer payment instruments. Therefore, while the scope of these rules is broader than some of the rules discussed earlier in this note, these rules can nonetheless be characterized as governing the over-the-air transmission of consumers' payment information.

[22] Payment Card Industry Security Standards Council, "PCI Payment Card Industry and Payment Application Device Data Security Standard Requirements and Security Assessment Procedures," version 1.2.1, § 2.1.1, p. 18 (July 2009).

[23] Payment Card Industry Security Standards Council, §1.2.3, p. 16.

[24] Payment Card Industry Security Standards Council, §6.1, p. 14.

[25]Payment Card Industry Security Standards Council, §§ 6.1(a) and 6.1(b), p. 14.

[26] Nev. Rev. Stat. Ann. §§ 603A.030, 603A.040, & 603A.215 (2010).

[27] "Data collector" is defined under the statute as "any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information." (See Nev. Rev. Stat. Ann. §§ 603A.215 (2010)).

[28] Nev. Rev. Stat. Ann. §§ 603A.215 (2010).

[29] Mass. Gen. Laws ch. 93H, §§ 1-6 (2007).

[30] 201 Mass. Code Regs. 17.00-17.05 (2009).

[31] This regulation applies to all "persons." "Person" is defined as "a natural person, corporation, association, partnership, or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof." See 201 Mass. Code Regs. 17.02 (2009).

[32] Under the regulations, the term "electronic" specifically includes wireless technology. "Electronic" is defined as "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities." See 201 Mass. Code Regs. 17.02 (2009).

[33] *See* 201 Mass. Code Regs. 17.02 (2009).

[34] 201 Mass. Code Regs. 17.00-17.05 (2009).

[35] 201 Mass. Code Regs. 17.04 (2009).

[36] Federal Financial Institutions Examination Council, "FFIEC 2010 Retail Payment Systems IT Examination Handbook," (2010), p. 40-41.

[37] Federal Financial Institutions Examination Council, (2010), p.41.

[38] See, for example, Robert L. Mitchell, "Hacking Contactless Payment Cards," *Computerworld*, June 11, 2007, noting that contactless consumer payment technology is generally safer than magnetic stripe technology.

[39] See, for example, Crowe et al. (May 17, 2010), p. 6, noting that "another advantage of contactless technology is that the chip can be used to store much more information [including information on warranties, reward programs, coupons, etc.] than can be stored on a magnetic stripe, and the information can be updated by a reader over the air."